

Topics in Error-Correcting Codes

Notes by Rohan Goyal

MIT — 6.S953

Lecture 11: Polynomial Codes

For this lecture, we broadly follow Prahladh Harsha's notes, linked below [1].

Reed–Muller Codes

Fix a finite field $\mathbb{F}_q$, a number of variables $m \geq 1$, and a degree bound $d \geq 0$. The *total degree* of a monomial $X_1^{e_1} \cdots X_m^{e_m}$ is $e_1 + \cdots + e_m$; the total degree of a nonzero polynomial is the largest degree of a monomial with nonzero coefficient.

On $\mathbb{F}_q$, the identity $X^q = X$ allows us to reduce each individual degree to at most $q - 1$ without changing any evaluations or increasing total degree. We therefore work with *reduced* polynomials

$$P(X_1, \dots, X_m) = \sum_{\substack{0 \leq e_i \leq q-1 \\ e_1 + \cdots + e_m \leq d}} c_{e_1, \dots, e_m} X_1^{e_1} \cdots X_m^{e_m}.$$

Definition 1 (Reed–Muller code). The code $\text{RM}_q(m, d)$ consists of the evaluation vectors

$$\text{Enc}(P) = (P(a))_{a \in \mathbb{F}_q^m},$$

where $P \in \mathbb{F}_q[X_1, \dots, X_m]$ is reduced and has total degree at most d . We fix an ordering of $\mathbb{F}_q^m$.

Proposition 2 (Length and dimension). *The code $\text{RM}_q(m, d)$ is $\mathbb{F}_q$ -linear, has length $n = q^m$, and has dimension*

$$K_q(m, d) = \# \left\{ (e_1, \dots, e_m) \in \{0, \dots, q-1\}^m : \sum_{i=1}^m e_i \leq d \right\}.$$

Proof. Evaluation is linear. To show that the allowed monomial evaluations are independent, it suffices to prove that a reduced polynomial vanishing on all of $\mathbb{F}_q^m$ is zero. For $m = 1$, this is the univariate root bound. In general, write the polynomial as a polynomial in X_m with coefficients in the other variables. After fixing those variables, the resulting polynomial has degree at most $q - 1$ and vanishes at all q field elements, so every coefficient vanishes. Induction on m now shows that each coefficient polynomial is zero. Hence evaluation is injective, and the dimension is the number of allowed monomials. $\square$

In particular, the q^m reduced monomials form a basis for all functions $\mathbb{F}_q^m \rightarrow \mathbb{F}_q$. Thus every such function has a unique reduced polynomial representation. The interesting degree range is $0 \leq d \leq m(q - 1)$.

The Low-Degree Case

Assume $0 \leq d < q$. The individual-degree constraints impose no additional restriction, so stars and bars gives

$$K_q(m, d) = \binom{m+d}{d}.$$

For $m = 1$ we recover the Reed–Solomon code of degree at most d evaluated at all q field elements. For $m = 2$ and $d = 2 < q$, a message specifies the six coefficients of

$$P(X, Y) = c_{00} + c_{10}X + c_{01}Y + c_{20}X^2 + c_{11}XY + c_{02}Y^2.$$

Its codeword contains q^2 evaluations. Notice that a total-degree bound of 2 excludes X^2Y^2 , even though each individual degree is 2.

The Schwartz–Zippel lemma

The univariate root bound says that a nonzero degree- d polynomial has at most d roots. In several variables, a polynomial can vanish on a whole hyperplane. The right statement bounds the *fraction* of zeros.

Lemma 3 (Schwartz–Zippel / polynomial distance lemma). *Let $P \in \mathbb{F}[X_1, \dots, X_m]$ be a nonzero polynomial of total degree at most d , and let $S \subseteq \mathbb{F}$ be finite and nonempty. Then*

$$\Pr_{a \in S^m} [P(a) = 0] \leq \frac{d}{|S|}.$$

Proof. If $d \geq |S|$, the bound is immediate, so assume $d < |S|$. Induct on m . For $m = 1$, this is the univariate root bound. Write

$$P(X_1, \dots, X_m) = \sum_{j=0}^r P_j(X_1, \dots, X_{m-1})X_m^j, \quad P_r \neq 0.$$

Since $\deg P_r \leq d - r$, the induction hypothesis gives

$$\Pr_{a' \in S^{m-1}} [P_r(a') = 0] \leq \frac{d-r}{|S|}.$$

If $P_r(a') \neq 0$, then $P(a', X_m)$ is a nonzero univariate polynomial of degree r , so it vanishes at at most r choices of $a_m \in S$. Splitting according to whether $P_r(a') = 0$ gives

$$\Pr[P(a) = 0] \leq \frac{d-r}{|S|} + \frac{r}{|S|} = \frac{d}{|S|}.$$

□

Corollary 4 (Low-degree Reed–Muller parameters). *For $0 \leq d < q$, the code $\text{RM}_q(m, d)$ has parameters*

$$\boxed{n = q^m, \quad k = \binom{m+d}{d}, \quad \delta = 1 - \frac{d}{q}.$$

Proof. For distinct polynomials P, Q of total degree at most d , apply Lemma 3 to $P - Q$. They disagree on at least a $1 - d/q$ fraction of points. This also proves injectivity of evaluation. To attain the bound, choose distinct $\alpha_1, \dots, \alpha_d \in \mathbb{F}_q$ and take

$$P(X_1, \dots, X_m) = \prod_{i=1}^d (X_1 - \alpha_i).$$

This polynomial is nonzero at exactly a $1 - d/q$ fraction of points. For $d = 0$, use the constant polynomial 1. $\square$

The length can now exceed the alphabet size: $n = q^m$, while each symbol is still in $\mathbb{F}_q$. The rate is $\binom{m+d}{d}/q^m$. In particular, with q, d fixed and m growing, the rate tends to zero. We next consider the binary field and then allow the degree to be larger than the field size.

A Brief Look at the Binary Case

Over $\mathbb{F}_2$, every field element satisfies $x^2 = x$. Consequently, every function on $\mathbb{F}_2^m$ has a unique multilinear representation, and the code $\text{RM}_2(m, d)$, for $0 \leq d \leq m$, consists of evaluations of

$$P(X) = \sum_{\substack{S \subseteq \{1, \dots, m\} \\ |S| \leq d}} c_S \prod_{i \in S} X_i.$$

Theorem 5 (Binary Reed–Muller parameters). *For integers $m \geq 1$ and $0 \leq d \leq m$, the binary Reed–Muller code $\text{RM}_2(m, d)$ has parameters*

$$n = 2^m, \quad k = \sum_{j=0}^d \binom{m}{j}, \quad \delta = 2^{-d}.$$

Proof. The block length is 2^m . There are $\sum_{j=0}^d \binom{m}{j}$ multilinear monomials of degree at most d , and uniqueness of multilinear representations makes evaluation injective. This gives the dimension.

Since the code is linear, its relative distance is the minimum fraction of nonzero coordinates in a nonzero codeword. Let $P \neq 0$ have degree $r \leq d$. After relabeling variables, suppose $X_1 \cdots X_r$ is a monomial of P with nonzero coefficient. Fix $X_{r+1}, \dots, X_m$ arbitrarily. The coefficient of $X_1 \cdots X_r$ remains 1: any other monomial containing all these variables would have degree greater than r . Thus the restricted polynomial is a nonzero multilinear polynomial in r variables. By uniqueness of multilinear representations, it has a nonzero evaluation at some choice of $X_1, \dots, X_r$. For every assignment to the remaining variables, at least a 2^{-r} fraction of choices of the first r variables therefore give a nonzero evaluation. Hence

$$\Pr_{a \in \mathbb{F}_2^m} [P(a) \neq 0] \geq 2^{-r} \geq 2^{-d}.$$

Finally, $X_1 \cdots X_d$ is nonzero on exactly a 2^{-d} fraction of points, attaining the bound. For $d = 0$, take the constant polynomial 1. $\square$

The Distance of General Reed–Muller Codes

The low-degree and binary distance bounds have a common generalization. We continue to use reduced polynomials, now allowing $d \geq q$.

Theorem 6 (General Reed–Muller distance). *Let $m \geq 1$ and $0 \leq d < m(q-1)$. Write*

$$d = s(q-1) + t, \quad 0 \leq t < q-1.$$

Then $\text{RM}_q(m, d)$ has relative distance

$$\delta = \frac{q-t}{q^{s+1}}.$$

For $d \geq m(q-1)$, the code is all of $\mathbb{F}_q^m$ and has relative distance q^{-m} .

Duals of Reed–Muller Codes

For evaluation vectors, the standard inner product is

$$\langle \text{Enc}(P), \text{Enc}(Q) \rangle = \sum_{a \in \mathbb{F}_q^m} P(a)Q(a) \in \mathbb{F}_q.$$

The key fact is cancellation when we sum a low-degree monomial over all field elements.

Lemma 7 (Sums of powers). *For $0 \leq j \leq q-1$,*

$$\sum_{a \in \mathbb{F}_q} a^j = \begin{cases} 0, & 0 \leq j < q-1, \\ -1, & j = q-1. \end{cases}$$

Here $a^0 = 1$, including when $a = 0$.

Proof. At $j = 0$, the sum is $q \cdot 1 = 0$ in $\mathbb{F}_q$. At $j = q-1$, every nonzero field element contributes 1, so the sum is $(q-1) \cdot 1 = -1$. For $0 < j < q-1$, let η generate $\mathbb{F}_q^*$. Multiplication by η permutes the field, giving

$$\sum_a a^j = \sum_a (\eta a)^j = \eta^j \sum_a a^j.$$

Since $\eta^j \neq 1$, the sum must be zero. □

Theorem 8 (Reed–Muller duality). *For $0 \leq d < m(q-1)$,*

$$\text{RM}_q(m, d)^\perp = \text{RM}_q(m, m(q-1) - d - 1).$$

Proof. Write $M = m(q-1)$. First consider monomials X^e and X^f of total degrees at most d and $M-d-1$, respectively. Then $\sum_i (e_i + f_i) \leq M-1$, so some coordinate i satisfies $e_i + f_i < q-1$. Factoring the sum and applying the lemma gives

$$\sum_{a \in \mathbb{F}_q^m} a_1^{e_1+f_1} \cdots a_m^{e_m+f_m} = \prod_{i=1}^m \left(\sum_{a_i \in \mathbb{F}_q} a_i^{e_i+f_i} \right) = 0.$$

By linearity, the two codes are orthogonal. Hence

$$\text{RM}_q(m, M - d - 1) \subseteq \text{RM}_q(m, d)^\perp.$$

It remains to match dimensions. Complementing exponents,

$$(e_1, \dots, e_m) \mapsto (q - 1 - e_1, \dots, q - 1 - e_m),$$

is a bijection from reduced monomials of total degree at least $d + 1$ to those of total degree at most $M - d - 1$. Therefore

$$K_q(m, M - d - 1) = q^m - K_q(m, d) = \dim(\text{RM}_q(m, d)^\perp).$$

Since $\text{RM}_q(m, M - d - 1)$ is contained in $\text{RM}_q(m, d)^\perp$ and the two spaces have the same dimension, they are equal. $\square$

Reminder: Familiar Binary Codes

Recall the following codes and duality relations from Problem Set 1.

Hadamard codes

For $d = 0$, $\text{RM}_2(m, 0)$ is the repetition code. For $d = 1$, the polynomials are affine linear functions

$$P_{b,u}(a) = b + u \cdot a, \quad b \in \mathbb{F}_2, \quad u \in \mathbb{F}_2^m.$$

Thus $\text{RM}_2(m, 1)$ has parameters

$$n = 2^m, \quad k = m + 1, \quad \delta = \frac{1}{2}.$$

These are the affine Hadamard codewords. Restricting to $b = 0$ gives the Hadamard code, of dimension m and relative distance $1/2$. Puncturing at $a = 0$ gives the punctured Hadamard code, with parameters

$$\boxed{n = 2^m - 1, \quad k = m, \quad \delta = \frac{2^{m-1}}{2^m - 1}.$$

Extended Hamming and Hamming codes

For $m \geq 2$, duality gives

$$\text{RM}_2(m, 1)^\perp = \text{RM}_2(m, m - 2).$$

Its parameters are

$$\boxed{n = 2^m, \quad k = 2^m - m - 1, \quad \delta = 2^{2-m}.$$

This is the *extended Hamming code*. Puncturing at $a = 0$ gives the *Hamming code*, with parameters

$$\boxed{n = 2^m - 1, \quad k = 2^m - m - 1, \quad \delta = \frac{3}{2^m - 1}.$$

Its dual is the punctured Hadamard code.

Two Univariate Extensions

Both codes below have block length n and alphabet $\mathbb{F}_q^s$. The message polynomial has degree less than k . Relative distance is the fraction of coordinates at which the *whole tuples* differ.

Definition 9 (Order- s univariate multiplicity code). Fix integers $s, n \geq 1$ and $1 \leq k \leq sn$, and distinct evaluation points $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$. Assume $\text{char}(\mathbb{F}_q) \geq s$. The order- s univariate multiplicity code, UMULT, encodes $P \in \mathbb{F}_q[X]$ with $\deg P < k$ by

$$\text{Enc}_{\text{UMULT}}(P)_i = (P(\alpha_i), P'(\alpha_i), \dots, P^{(s-1)}(\alpha_i)), \quad 1 \leq i \leq n,$$

where $P^{(j)}$ is the usual j th formal derivative and $P^{(0)} = P$ [3].

Definition 10 (Order- s folded Reed–Solomon code). Fix integers $s, n \geq 1$ and $1 \leq k \leq sn$, a nonzero $\gamma \in \mathbb{F}_q$, and evaluation points $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ satisfying, for every i, j and $0 \leq t < s$,

$$\alpha_i \gamma^t = \alpha_j \iff i = j \text{ and } t = 0.$$

The order- s folded Reed–Solomon code, FRS, encodes $P \in \mathbb{F}_q[X]$ with $\deg P < k$ by

$$\text{Enc}_{\text{FRS}}(P)_i = (P(\alpha_i), P(\alpha_i \gamma), \dots, P(\alpha_i \gamma^{s-1})), \quad 1 \leq i \leq n.$$

The separation condition makes all sn evaluation points distinct [2, Section 17.1].

Theorem 11 (Rate and relative distance of UMULT and FRS). *Under their respective hypotheses, both order- s codes have q^k codewords, block length n , alphabet $\mathbb{F}_q^s$, and*

$$\boxed{R = \frac{k}{sn}, \quad \delta = 1 - \frac{1}{n} \left\lfloor \frac{k-1}{s} \right\rfloor.}$$

References and Further Reading

- [1] Prahladh Harsha. [Coding Theory, Lecture 8](#). Tata Institute of Fundamental Research, September 21, 2022. Reed–Muller portion, pages 3–8.
- [2] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. [Essential Coding Theory](#). Draft of August 26, 2025. Sections 9.1–9.4 for Reed–Muller codes and their distance, and Section 17.1 for folded Reed–Solomon codes.
- [3] Swastik Kopparty. [Some remarks on multiplicity codes](#). arXiv:1505.07547, 2015.